# On Bad Reduction of Elliptic Curves

by

Loren D. Olson

The purpose of this note is to show how the coefficients of the canonical invariant differential on an elliptic curve $C$ defined over the field $\mathbb{Q}$ of rational numbers may be used to determine the type of reduction at a prime $p$ where $C$ has bad reduction. Simple and explicit formulas for these coefficients are obtained. This also yields on easy method for calculating the local L-functions at these primes. To do this we use a theorem of Honda [2,3] which says that the formal group $F$ of the curve $C$ is strongly isomorphic over $\mathbb{Z}$ to the formal group $G$ associated to the global L-series of $C$. We then proceed to analyse the singularity of the reduced curve and obtain the desired formulas.

## § 1. Introduction.

All curves, points, etc. in this paper will be assumed to be defined over $\mathbb{Q}$. Let $C$ be an elliptic curve. Then $C$ has an affine Weierstrass minimal model of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.1}$$

with $a_i \in \mathbb{Z}$, and a corresponding projective model

$$Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \qquad (1.2)$$

The $\mathbb{Q}$-rational point $e = (0,1,0)$ is the identity element for the group law on $C$. If $C$ has good reduction at a prime $p$ and $f_p$ denotes the trace of Frobenius $F_p$ at $p$, then the characteristic polynomial of $F_p$ is $1 - f_pt + pt^2$. If $C$ has bad reduction at $p$ and the singularity is a cusp, let $f_p = 0$. In this case the non-singular part of $C$ is isomorphic over $\mathbb{Z}/p\mathbb{Z}$ to the additive group $G_a$ and we have <u>additive reduction</u>. If $C$ has bad reduction at $p$ and the singularity is a node with the two tangents rational over $\mathbb{Z}/p\mathbb{Z}$, let $f_p = 1$. Then the non-singular part of $C$ is isomorphic over $\mathbb{Z}/p\mathbb{Z}$ to the multiplicative group $G_m$ and we have <u>split multiplicative reduction</u>. If $C$ has bad reduction at $p$ and the singularity is a node with the two tangents not rational over $\mathbb{Z}/p\mathbb{Z}$, let $f_p = -1$. In this case the non-singular part of $C$ is isomorphic over a quadratic extension of $\mathbb{Z}/p\mathbb{Z}$ to the multiplicative group $G_m$ and we have <u>non-split multiplicative reduction</u>. We wish to derive some simple arithmetical criteria for determining which of these three types of reduction occurs at a given prime $p$ where $C$ has bad reduction.

The <u>local L-function</u> $L_p(s)$ <u>of</u> $C$ <u>at</u> $p$ is defined as $L_p(s) = (1-f_pp^{-s}+p^{1-2s})^{-1}$ if $C$ has good reduction at $p$, and $L_p(s) = (1-f_pp^{-s})^{-1}$ if $C$ has bad reduction at $p$. The <u>global L-function of</u> $C$ is $L(s) = \prod_p L_p(s)$. We want to use the following result of Honda [2,3] in our investigations.

<u>Theorem 1.1 (Honda)</u>. The formal group $F$ of $C$ is strongly isomorphic over $\mathbb{Z}$ to the formal group $G$ associated to the global

L-function of $C$ .

Let $\omega$ be the canonical invariant differential on $C$ and $C_{p-1}$ the coefficient of $Z^{p-1}$ in the expansion of $\omega/dZ$ . An immediate consequence of Honda's theorem is that $f_p$ is congruent to $C_{p-1}$ modulo $p$ .

Corollary 1.2. Let $C$ be an elliptic curve, and assume that $C$ has bad reduction at a prime $p$ . Then

(1) $C_{p-1} \equiv 0,1,-1 \pmod{p}$

(2) $C$ has additive reduction at $p \iff C_{p-1} \equiv 0 \pmod{p}$

(3) $C$ has split multiplicative reduction at $p \iff C_{p-1} \equiv 1 \pmod{p}$

(4) $C$ has non-split multiplicative reduction at $p \iff C_{p-1} \equiv -1 \pmod{p}$ and $p > 2$ .

Proof: Since $C_{p-1} \equiv f_p \pmod{p}$ and $f_p = 0,1$ , or $-1$ , the congruence class of $C_{p-1}$ modulo p determines the reduction type uniquely as indicated except for $p = 2$ . But since all polynomials of degree 2 are reducible over $\mathbb{Z}/2\mathbb{Z}$ (and, in particular, the one giving the tangents at the singular point), the only possible type of multiplicative reduction is split multiplicative reduction.

Thus we see that the residue class of $C_{p-1}$ modulo p determines the type of reduction modulo p . We would like to have more information concerning $C_{p-1}$ and $f_p$ .

Define the following invariants of a model for $C$ of the form (1.1): $b_2 = a_1^2+4a_2$ , $b_4 = a_1a_3+2a_4$ , and $c_4 = b_2^2-24b_4$ . $b_2$ and $b_4$ correspond to Neron's $\bar{\alpha}$ and $\bar{\beta}$ [4,p.450]. As we

shall see, $c_4$ is a sufficiently good invariant to distinguish between additive and multiplicative reduction, but it is not fine enough to separate split and non-split multiplicative reduction, i.e. to distinguish between $f_p = 1$ and $f_p = -1$ and thus to determine the local L-function completely.

From now on we shall assume that $C$ has bad reduction at the prime $p$ under discussion.

## § 2. The case $p = 2$

Since $C_{p-1}$ modulo p determines the type of reduction at p , we want to compute $C_{p-1}$ , in this case $C_1$ . For a curve given in the form (1.1) or, equivalently, (1.2), we have

$$\omega = dX/(2Y+a_1X+a_3) \tag{2.1}$$

Expressing $X$ and $Y$ in terms of $Z$ and computing (cf. Tate [5] for the details), one obtains

$$C_1 = a_1 \tag{2.2}$$

Theorem 2.1. (1) $C$ has additive reduction at $2 \iff a_1 \equiv 0 \pmod 2 \iff c_4 \equiv 0 \pmod 2$

(2) $C$ has split multiplicative reduction at $2 \iff a_4 \not\equiv 0 \pmod 2 \iff c_4 \not\equiv 0 \pmod 2$

Proof: $c_4 = b_2^2-24b_4 \equiv b_2^2 \equiv b_2 \equiv a_1^2+4a_2 \equiv a_1^2 \equiv a_1 \equiv C_1 \pmod 2$. Applying Corollary 1.2 completes the proof.

## § 3. The case $p = 3$

As in § 2, a short computation (again see Tate [5] for the details) yields

$$c_2 = a_1^2+a_2 \tag{3.1}$$

Theorem 2.2. (1) $C$ has additive reduction at $3 \iff a_1^2+a_2 \equiv 0 \pmod 3 \iff c_4 \equiv 0 \pmod 3$ .

(2) $C$ has multiplicative reduction at $3 \iff a_1^2+a_2 \not\equiv 0 \pmod 3 \iff c_4 \not\equiv 0 \pmod 3$ .

(3) $C$ has split multiplicative reduction at $3 \iff a_1^2+a_2 \equiv 1 \pmod 3$

(4) $C$ has non-split multiplicative reduction at $3 \iff a_1^2+a_2 \equiv -1 \pmod 3$ .

Proof: $c_4 \equiv b_2^2-24b_4 \equiv b_2^2 \equiv (a_1^2+4a_2)^2 \equiv (a_1^2+a_2)^2 \pmod 3$ .

The theorem then follows immediately from formula (3.1) and Corollary 1.2.

Remark. $c_2^2 \equiv c_4 \pmod 3$ . Note that $c_2 = a_1^2+a_2$ is a more sensitive invariant than $c_4$ in that the residue class of $c_2$ modulo 3 allows us to distinguish between split and non-split multiplicative reduction, while $c_4$ does not allow us to separate these two possibilities.

## § 4. The case $p \geq 5$

Assume $p \geq 5$ . Then there exists an affine minimal model for $C$ at $p$ of the form

$$Y^2 = X^3+AX+B \tag{4.1}$$

with $A, B \in \mathbb{Z}$ . The coefficient $C_{p-1}$ modulo $p$ is given by Deuring's classical formula [1]

$$C_{p-1} \equiv \sum_{2h+3i=P} \frac{P!}{i!h!(P-h-i)!} A^h B^i \pmod{p} \tag{4.2}$$

where $P = (1/2)(p-1)$ .

Let $S = (x,y)$ be the singular point on the reduced curve with $x,y \in \mathbb{Z}/p\mathbb{Z}$ . The tangents at $S$ are given by a quadratic polynomial $R(T)$ as follows: Transform the curve by $X \mapsto (X+x)$, $Y \mapsto (Y+y)$ so that the singularity is now at $(0,0)$ . The tangents are given by a homogeneous form of degree 2 in $X$ and $Y$ which we can consider as a quadratic polynomial $R(T)$ with $T = Y/X$ . Let $D$ be the discriminant of $R(T)$ , and let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol with respact to $p$ .

Proposition 4.1. (1) $C$ has additive reduction at $p \iff f_p = 0 \iff S$ is a cusp $\iff R(T)$ has two identical roots over $\mathbb{Z}/p\mathbb{Z} \iff D = 0 \iff (\frac{D}{p}) = 0$ .

(2) $C$ has split multiplicative reduction at $p \iff f_p = 1 \iff S$ is a node with rational tangents $\iff R(T)$ has two distinct roots rational over $\mathbb{Z}/p\mathbb{Z} \iff (\frac{D}{p}) = 1$ .

(3) $C$ has non-split multiplicative reduction at $p \iff f_p = -1 \iff S$ is a node with irrational tangents $\iff R(T)$ has two distinct roots not rational over $\mathbb{Z}/p\mathbb{Z} \iff (\frac{D}{p}) = -1$ .

Corollary 4.2. $f_p = \left(\frac{D}{p}\right)$ .

Let

$$H = Y^2-X^3-AX-B \tag{4.3}$$

Then we have

$$\partial H/\partial X = -3X^2-A \tag{4.4}$$

$$\partial H/\partial Y = 2Y \tag{4.5}$$

From (4.5) we must have $y = 0$ . From (4.4) we must have $x^2 = -A/3$ in $\mathbb{Z}/p\mathbb{Z}$ , so that $-A/3$ is either a quadratic residue modulo p or 0 modulo p . Note that $x = 0 \iff A \equiv 0 \pmod p$ . Let $X^3-AX-B = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ be a factorization over $\mathbb{Z}/p\mathbb{Z}$ . At least two of $\alpha_1$, $\alpha_2$, $\alpha_3$ must coincide with $x$ , let us say $x = \alpha_2 = \alpha_3$ . Then

$$X^3+AX+B = X^3+(-\alpha_1-2\alpha_2)X^2+(2\alpha_1\alpha_2+\alpha_2^2)X-\alpha_1\alpha_2^2 \tag{4.6}$$

Thus comparing coefficients, we have

$$0 = -\alpha_1-2\alpha_2 \tag{4.7}$$

$$A = 2\alpha_1\alpha_2+\alpha_2^2 \tag{4.8}$$

$$B = -\alpha_1\alpha_2^2 \tag{4.9}$$

Hence

$$\alpha_1 = -2\alpha_2 \tag{4.10}$$

$$A = 2\alpha_1\alpha_2+\alpha_2^2 = -3\alpha_2^2 = -3x^2 \tag{4.11}$$

$$B = -\alpha_1\alpha_2^2 = 2\alpha_2^3 = 2x^3 \tag{4.12}$$

From (4.12) we see that $B/2$ is either a cubic residue modulo p or 0 modulo p . Note that $x = 0 \iff B \equiv 0 \pmod p$ from (4.12).

Transform the curve by $X \mapsto (X+\alpha_2)$ , $Y \mapsto Y$ so that the singular point $S = (x,y) = (x,0) = (\alpha_2,0)$ goes to $(0,0)$ . We obtain

$$Y^2-(X+\alpha_2)^3-A(X+\alpha_2)-B = Y^2-X^3-3\alpha_2X^2 \qquad (4.13)$$

The tangents to $(0,0)$ on the transformed curve are given by

$$Y^2-3\alpha_2X^2 = 0 \qquad (4.14)$$

so that the polynomial $R(T)$ is $R(T) = T^2-3\alpha_2$ . $D = 12\alpha_2 = 12x$ . $c_4 = b_2^2-24b_4 = (a_1^2+4a_2)^2-24(a_1a_3+2a_4) = -48A$ . Since $x = 0 \iff A \equiv 0 \pmod p$ , $D = 0 \iff A \equiv 0 \pmod p$ and so the invariant $c_4$ is enough to distinguish between additive and multiplicative reduction. However, as we shall see below it does not separate split and non-split multiplicative reduction.

Theorem 4.3. (1) $C$ has additive reduction at $p \iff A \equiv 0 \pmod p \iff B \equiv 0 \pmod p \iff (\frac{-2AB}{p}) = 0$ .

(2) $C$ has split multiplicative reduction at $p \iff (\frac{-2AB}{p}) = 1$ .

(3) $C$ has non-split multiplicative reduction at $p \iff (\frac{-2AB}{p}) = -1$.

Proof: (1) We have seen that $A \equiv 0 \pmod p \iff x = 0 \iff B \equiv 0 \pmod p$ . $C$ has additive reduction at $p \iff D = 12x = 0 \iff x = 0 \iff A \equiv B \equiv 0 \pmod p \iff (\frac{-2AB}{p}) = 0$ .

(2) and (3) From (4.14) we see that $C$ has split multiplicative reduction at $p \iff 3\alpha_2$ is a non-zero square in $\mathbb{Z}/p\mathbb{Z}$ and that $C$ has non-split multiplicative reduction at $p \iff 3\alpha_2$ is not a square in $\mathbb{Z}/p\mathbb{Z}$ . From formulas (4.11) and (4.12) we have that $3\alpha_2 = (-9/2)B/A$ . Thus $3\alpha_2$ is a square $\iff (-9/2)B/A$ is a square modulo $p \iff -2AB$ is a square modulo $p \iff (\frac{-2AB}{p}) = 1$ .

Corollary 4.4. $f_p = \left(\frac{-2AB}{p}\right)$ .

## § 5. Examples

Given an elliptic curve $C$ in the form of a minimal model (1.1) or (1.2), one computes the bad primes by finding the divisors of the discriminant $\Delta = -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6$ where $b_6 = a_3^2+4a_6$ and $b_8 = b_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2$ . We can then apply the methods of the preceding sections to determine $f_p$ and hence the type of reduction.

Example 5.1. Let $C$ be given by $Y^2 = X^3+X+1$ . This equation is minimal. The discriminant is $\Delta = -16(31)$ , so $C$ has bad reduction at $p = 2$ and $p = 31$ . For $p = 2$ , $C_{p-1} = C_1 = a_1 = 0$ , so we have additive reduction at $p = 2$ . For $p = 31$ , we can apply Theorem 4.3 and Corollary 4.4. $f_p = \left(\frac{-2AB}{p}\right) = \left(\frac{-2}{31}\right) = -1$ , so that $C$ has non-split multiplicative reduction at $p = 31$ . Alternatively, one may use Deuring's formula to compute $C_{p-1}$ . A third possibility, of course, is to factor $X^3+X+1$ over $\mathbb{Z}/31\mathbb{Z}$ and then analyse (4.14). $c_4 = -48$ .

Example 5.2. Let $C$ be given by $Y^2 = X^3+X-1$ . The equation is minimal and $\Delta = -16(31)$ . We have additive reduction at $p = 2$ since $C_{p-1} = C_1 = a_1 = 0$ . For $p = 31$ , $f_p = \left(\frac{-2AB}{p}\right) = \left(\frac{2}{31}\right) = 1$ , so that $C$ has split multiplicative reduction at $p = 31$ . $c_4 = -48$ .

Remark. Comparing examples 5.1 and 5.2, one sees that $c_4$ is the same in both cases. However, 5.1 exhibits non-split multiplicative

reduction at $p = 31$ , while 5.2 exhibits split multiplicative reduction at the same prime.

Example 5.3. Let $C$ be given by $Y^2 = X^3+7X+5$ . The equation is minimal and $\Delta = -16(23)(89)$ . $C$ has bad reduction at $p = 2,23$ , and $89$ . For $p = 2$ , $C_{p-1} = C_1 = a_1 = 0$ , so we have additive reduction at $p = 2$ . For $p = 23$ , we have $f_p = (\frac{-2AB}{p}) = (\frac{-70}{23}) = (\frac{-1}{23}) = -1$ , so that $C$ has non-split multiplicative reduction at $p = 23$ . For $p = 89$ , we have $f_p = (\frac{-2AB}{p}) = (\frac{-70}{89}) = (\frac{19}{89}) = -1$ , so that $C$ has non-split multiplicative reduction at $p = 89$ as well.

Remark. The computation of the Legendre symbol is much easier to carry out in practice than either the computation of $C_{p-1}$ via Deuring's formula or by searching for roots of the polynomial $X^3+AX+B$ .

## Bibliography

1) Deuring, M., Die Typen der Multiplikatorenringe elliptischer Functionenkörper, Abh.Math.Sem. Univ. Hamburg 14 (1941), 197-272.

2) Honda, T., Formal groups and zeta functions, Osaka J. Math. 5 (1968), 199-213.

3) Honda, T., On the theory of commutative formal groups, J.Math.Soc. Japan 22 (1970), 213-246.

4) Neron, A., Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, IHES, Publ.Math. 1964, 361-483.

5) Tate, J., The arithmetic of elliptic curves, Colloquium Lectures, Dartmouth College, Hanover, New Hampshire, August 29 - September 1, 1972.